ABSTRACT

An encryptor/ decryptor capable of achieving secure cryptographic communication by applying appropriate padding to a cryptosystem such as NTRU cryptosystems.

When an n-bit plaintext M is received, the OAEP + padding is applied thereto. According to a conversion rule or a conversion function A that satisfies the conditions as described below, two bit strings m and r are obtained from the result of the OAEP + padding. The conversion function A is a map to map a bit string consisting of k bits or less to the element of $L_m \times L_r$, where L_m is the scope of m and L_r is the scope of r. The conversion function A should satisfy the following conditions: A is injective; A and the inverse map thereof can be computed by a polynomial time; and if an encryption function is denoted by E(m, r), a map E: $A(X) \rightarrow L_e$ is a one-way function, where X is the scope of (m, r) and L_e is the space of the entire ciphertext. After a bit string is divided into the two bit strings m and r, $e = E^r(m)$ is computed to be encrypted. Thus, a ciphertext e is transmitted to a receiver.